CorreLog®

Correlation Session Monitor

Users Manual

http://www.correlog.com mailto:info@correlog.com

CorreLog, Correlation Session Monitor

Copyright © 2008 - 2015, CorreLog, Inc. All rights reserved.

No part of this manual shall be reproduced without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibilities for errors or omissions. Nor is any liability assumed for damages resulting from the use of this information contained herein.

Table of Contents

Section 1: Introduction …….. 5

Section 2: Software Installation …….. 9

Section 3: Software Operation …….. 13

Section 4: Advanced Usage …….. 23

Alphabetical Index …….. 31

Section 1: Introduction

This manual provides a detailed description of the CorreLog Correlation Session Monitor Plug-in software. This is an optional set of files and executables added to the CorreLog Server to track user logins (and other sessions) that are delimited by well defined start and stop messages, such as login and logout messages.

The manual provides information on installation and usage of this software, as well as a detailed description of screens, and certain features not documented elsewhere within the CorreLog manual set.

The Correlation Session Monitor software consists of a new screen that is added to the system, located in the "Correlation > Sessions" tab. This new screen provides special capabilities to configure match patterns that identify start and stop points for messages, such as when a user logs into a platform and then logs out of the platform. This provides special capability to see what sessions are active, what users may have been available, and what sessions may have been conducted during a security event.

This manual is intended for CorreLog users who will operate the system, as well as system administrators responsible for installing the software components. This information will also be of interest to program developers and administrators who want to extend the range of the CorreLog system's role within an enterprise to include special alerting of sessions, including special logon management.

Background Information

The "Session Monitor" software operates on an abstract session, which is a series of messages delimited by a start and stop message. This idea of a session relates directly to system logons, but may also be applied to other abstractions, such as VPN sessions, maintenance sessions, or other time-interval spans that have well defined start and stop points. Two items identify each session:

- **Session IP Address.** A session (as defined by CorreLog) is always related to an IP address that sends the start and stop messages. For example, this is the IP address of the device that the user access via login and logout operations. The IP address can also be related to VPN gateways, or other network based devices.

- **Session ID.** A session (as defined by CorreLog) has a certain session ID that is parsed from the start message, and later used to identify the stop message. This session ID may be a user name, an IP address, or any single word or phrase that is contained in both the "start" and "stop" messages.

Any two messages that have the above criteria are sufficient to create and maintain a CorreLog session. If necessary, the "Session IP Address" may be further created using the IP address override function (discussed elsewhere); the session ID is generally known through simple inspection of the session start and stop messages, as discussed in Section 3 of this manual.

Session Monitor Operation

The software herein simplifies the analysis of sessions by recording their states, collecting data related to the "session running" state, and maintaining a history of sessions. The "Session Monitor" therefore simplifies a common activity of the operator, which is to determine what users may have been on a set of network devices at the time of a particular event

The CorreLog operator creates one or more session monitors via the "Correlation > Sessions" tab, which is a standard and familiar CorreLog dialog. Once created by the operator, each session monitor function operates as follows:

1. The CorreLog program looks for a "start session message" with a particular pattern, such as a login message, but possibly some other type of startup message (such as a connection message.)

2. When the start message is received, the program parses a particular word from the message (such as a user name) and records this value as the "session id" for the session, along with the IP address for the start

message. This value is available for use in the other fields through the special "$sessid" value.

3. The program then looks for and end message containing a particular pattern and the "session id" that was parsed above.

4. While the program is awaiting the end message, the Session monitor can tabulate other messages of interest (by default all messages with the specified session ID from the IP address, but potentially other messages as well.)

5. When the end message is received, the session information is recorded and stored in history for later review, and a message is sent back to CorreLog for further correlation and reporting.

Using this technique, the operator can see what sessions are currently active, and can review the session history, providing an easy technique to determine (for example) what users are currently logged into the system, how long they have been logged in, and what users were logged into the system at a particular past point in time.

Process Overview

The Session Monitor consists of a single background process that operates independent of the other standard processes. This is the "CO-sess.exe" process, which will appear in the Windows task manager of the CorreLog server when the process is installed. This process must be running in order to support the anomaly detection, and is normally started via the "System > Schedule" screen, as described in Section 2.

The "CO-sess.exe" process monitors the received logs (in a fashion similar to the standard "CO-catlog.exe" and "CO-devlog.exe" processes.) The process parses each message looking for a start message that matches a particular pattern. When a message is detected that contains this start pattern, the message is parsed to obtain the "Session ID" (described above.) The process records the start message time, and begins looking for an end message that matches and end pattern and Session ID, indicating the end of the session. When the end message is found, the session is recorded and added to the session history.

While the "CO-sess.exe" program is waiting for the end message, additional messages can be tabulated, providing a degree of statistical awareness about the session, such as the number of messages that match other patterns.

The list of current and historical sessions is viewed via a new screen, added as part of this package. The user can click the "Correlation > Sessions" tab to view

the different types of sessions, and can drill down into a session to view the actual keywords and counts.

The session data is stored in textual format within the "stat/sess.stt" file of the CorreLog server system. This file is updated within a few seconds of any change to the session data, and is agreeable to further scripting, such as via the "Custom Alerts" facility or other custom process.

How To Use This Manual

The next section of this manual (Section 2) provides the essential information needed to install, configure, and test the Session Monitor software. Note that the only required component of the system is the configuration screen. Other information on the CorreLog server can be found in the standard "User Manual", including operation and application notes that will be of assistance in processing the alerts and tickets generated by the program, and received by the CorreLog Syslog receiver process.

Section 2: Software Installation

The CorreLog Session Monitor software is usually delivered as a self-extracting WinZip file. The installation requires minimal installation steps. Basic installation steps are as follows:

1. The operator obtains the CorreLog Session Monitor software, in self-extracting WinZip format, and executes the self-extracting WinZip file. This unzips the software into the existing CorreLog Windows Distribution, including all configuration data and executables

2. The operator accesses the "Correlation > Sessions" tab (added by the installation procedure) and configures one or more session monitors. (These steps are described briefly in this section, with further elaboration in Section 3.)

3. The operator optionally tests the software using the "Post New Message" hyperlink found on the "Messages > Search" screen to verify the operation of the system and configuration of the Session Monitor.

Actual installation steps, as well as initial tests of the software, are documented in this section. The information needed to perform the comprehensive configuration of Session Monitor parameters is provided in Section 3, along with a description of system operation and application notes.

Administrative logins are required in order to perform the software installation. The detailed steps needed to perform the installation are provided in the sections that follow.

Installation Requirements

The Session Monitor software can be installed on a variety of platforms and operating systems, including Windows 2K, Windows 7, and Windows Vista operating systems. The following items are required.

- **Existing CorreLog Server Installation.** Prior to installing the Session Monitor software, the CorreLog Server system must be installed on a Windows platform, as discussed in the CorreLog User Reference Manual.

- **Disk Space Requirements.** The Session Monitor software requires no significant disk space beyond the normal footprint of the CorreLog server. There is generally no extra disk space load due to this software.

- **CPU Requirements**. The Session Monitor software requires very little extra CPU requirements. A single new persistent process is started the CorreLog Windows platform.

Windows Installation Procedure

The CorreLog Session Monitor package is simple to install. The user simply obtains the plug-in package, and executes the package to extract the plug-in components to the CorreLog installation, and then stops and restarts the CorreLog Framework Service. The specific steps needed to install and the software are as follows:

1. Login to the CorreLog Server Windows platform using an "Administrator" type login.

2. Stop the "CorreLog Framework Service" via the "net stop correlog" command, or via the Windows Service Manager, and make sure that all CorreLog processes are actually stopped via the Windows "Task Manager" program.

3. Obtain and execute the "co-n-n-n-sess.exe" package, extracting files to the directory location where CorreLog is installed (by default the location "C:\CorreLog").

   Note: A common mistake is to extract files to some directory other than the existing CorreLog installation. The user should make sure that the location of the CorreLog server (such as C:\CorreLog or D:\CorreLog) is correctly specified.

4. Restart the "CorreLog Framework Service" via the "net start correlog" command, or via the Windows Service Manager, and verify that the "CO-

sess.exe" process is now running via the Windows "Task Manager" program.

5. Log into the CorreLog web interface using a CorreLog "admin" type login, and access the CorreLog "Alerts" screen, by clicking the new "Correlation > Sessions" tab at the top of the display.

   Note: This tab is added to the system during step #2 above. If the tab does not exist, the operator probably extracted the files to the wrong directory. (For specific user help, see the next section of this manual.)

Preliminary Checkout And Test Procedure

By default, the Session Monitor comes preconfigured with match patterns that work with the Windows and UNIX agent programs. The operator can test the operation of this default session monitor by logging in and out of a managed computer that is running the agent program. This causes a session to start and end on the specified platform, as indicated by the "Correlation > Sessions" screen.

The operator can also test the operation of the session with test messages, using the "Post Message" screen of the "Messages > Search" screen to insert messages into the running log. This provides a simple stand-alone technique for verifying operation, as follows.

1. Generate a test message via the "Messages > Search" screen that contains the following specific text (in addition to any other text within the test message)

   New User Login - User Name: Test000 message

   This causes the "Test000" user to be added to the "Messages > Users" screen, and starts a new session, with the Session ID being the name "Test000".

2. Verify that a new session appears in the "Correlation > Session" screen for the "Test000" user. (Click on the "Active Sessions" link for the session monitor to view data.

3. To end the session, generate a test message via the "Messages > Search" screen that contains the following specific text (in addition to any other text within the test message)

   Login Monitor: User Logout Test000

   This causes the "Test000" user session to end.

4. Verify that the session has been removed from the "Active Sessions", and moved to "Session History". Further note that this causes a message to be send back to the event log indicating the end of the session, including the elapsed session time.

The above procedure furnishes a simple test and example of operation. The first message causes the Test000 Session ID to be recorded, whereas the second message causes that particular session to be ended. At any given time, there may be hundreds or thousands of different sessions running on the system. The Session Monitor tracks the existence of these sessions, and records their history.

The above procedure provides a cursory discussion of the session monitor operation. A complete discussion of Session Monitor operation is supplied in Section 3 of this manual.

Section 3: Software Operation

The CorreLog Session Monitor software comes pre-configured with a single session monitor that works with the CorreLog Windows and UNIX agent programs. This default configuration may be adequate for many locations. However, the software is intended to be a general-purpose tool for tracking a wide variety of different sessions, and can be configured by the user to report these different sessions as described in this section.

- **Configuration of Session Detection.** The software allows the operator to configure unique session monitors, necessary to detect the start and stop of sessions, using the "AddNew" and "Wizard" functions of the top-level screen. This allows the operator flexibility to craft session monitors for specific purposes outside the default configuration.

- **Collection And Browsing of Session Data.** The software allows the operator to interactively browse session data, including the currently active sessions, as well as session history. The operator can additionally view graphic depictions of the session data, and drill down to see the sessions that were active at any given time. The operator can optionally view the session data recorded in a database.

- **Advanced Session Detection Functions.** The software includes various techniques to perform automatic and advanced statistical analysis of session data, and report issues that may indicate a security problem, and create custom alerts on session anomalies.

Top-Level Sessions Screen

The top-level sessions screen is accessed via a new tab added to the system by the installation process. All session detection, reporting, and advanced functions are available from the "Correlation > Sessions" screen, depicted below.

CorreLog Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
CORRELOG
Search | Query | More
Home Dashboards Messages/ Correlation/ Alerts/ Tickets/ Reports/ System/ Help
Threads Sessions Triggers Associations Actions Config/
Sort By: Name Match: * Apply AddNew > Wizard > Advanced >
Edit: Session Monitor Name: Time Updated: Active Sess Count:
#01 All User Logon Sessions
Active Sessions | History | Graphs
2011/08/16 09:56:10
1
Total monitored sessions: 1 of 50000 available. (0% full.)
Audit Full Session Monitor Data
Copyright © 2008 - 2011, CorreLog, Inc. All rights reserved.
Screen Generation Time: 0.594 Seconds. - Go To Top... | Site Info...
Evaluation License - Expires 2011/09/15 17:08:48 (31 days)
Local intranet

As shown above, the "Correlation > Sessions" screen contains a single default session monitor, configured to work with the CorreLog Agent programs. The operator can add new sessions via the "AddNew" or "Wizard" buttons, and can edit or delete existing entries via the "Edit #NN" button to the left of each session. The default session may be adequate for many applications, however most users will create multiple session monitors to track the specific data items and sessions of their enterprise.

Screen Control Bar

At the top of the "Sessions" screen is a control bar that permits the user to sort, filter, and add new session monitors to the system. This screen control bar is similar to those found on other CorreLog screens. The main components of the control bar are described below.

- **Sort Mode.** The upper part of the display includes a "Sort Mode" that will sort the top-level list of sessions by Time, Name, and Count. This is useful when there are many different session monitors defined on the system.

- **Match Pattern.** The upper part of the display includes a "Match Pattern" (and "Apply" button) that can be used to filter the list of top-level session categories. The user can specify a keyword or wildcard to limit the display to matched session titles.

- **Add New Button. / Wizard Button** The upper part of the display contains an "Add New" and a "Wizard" button that will allow the user to add a new sessions to the system. (Specific configuration items are defined later in this section.)

- **Advanced Functions Button.** The upper part of the display contains an "Advanced" button that allows the user to access the advanced monitoring functions of the session monitor. (Specific configuration items are defined later in this section.)

Session Data Table

Beneath the control bar are zero or more session monitors, where each entry is created via the "AddNew" button, or "Wizard" button

The user can configure many different session monitors, but the total number of sessions collected by the system is limited to 50,000 (unless otherwise modified by CorreLog support.) The total number sessions in the system, and the percent capacity of the system, is listed at the bottom of the screen.

Each session monitor has the following specific data items:

- **Session Title.** Each session monitor has a title that is defined by the user, which describes the purpose and intent of the monitor. The title can be matched via the "Match Pattern" (described above), and is incorporated into any self-generated alerts. The title is completely arbitrary, but is usually reflective of the type of session being monitored.

- **Active Sessions / History / Graphs Links.** Each session monitor has links that can be used to display the currently active sessions (if any) the session history, and display a graphical depiction of the session history. The user clicks on any of these links to see the actual session data collected by the monitor.

- **Time Updated.** Each session monitor reports the time that the monitor was last updated, to the immediate right of the session monitor title. The user can sort on these items to see which session monitors were more recently updated.

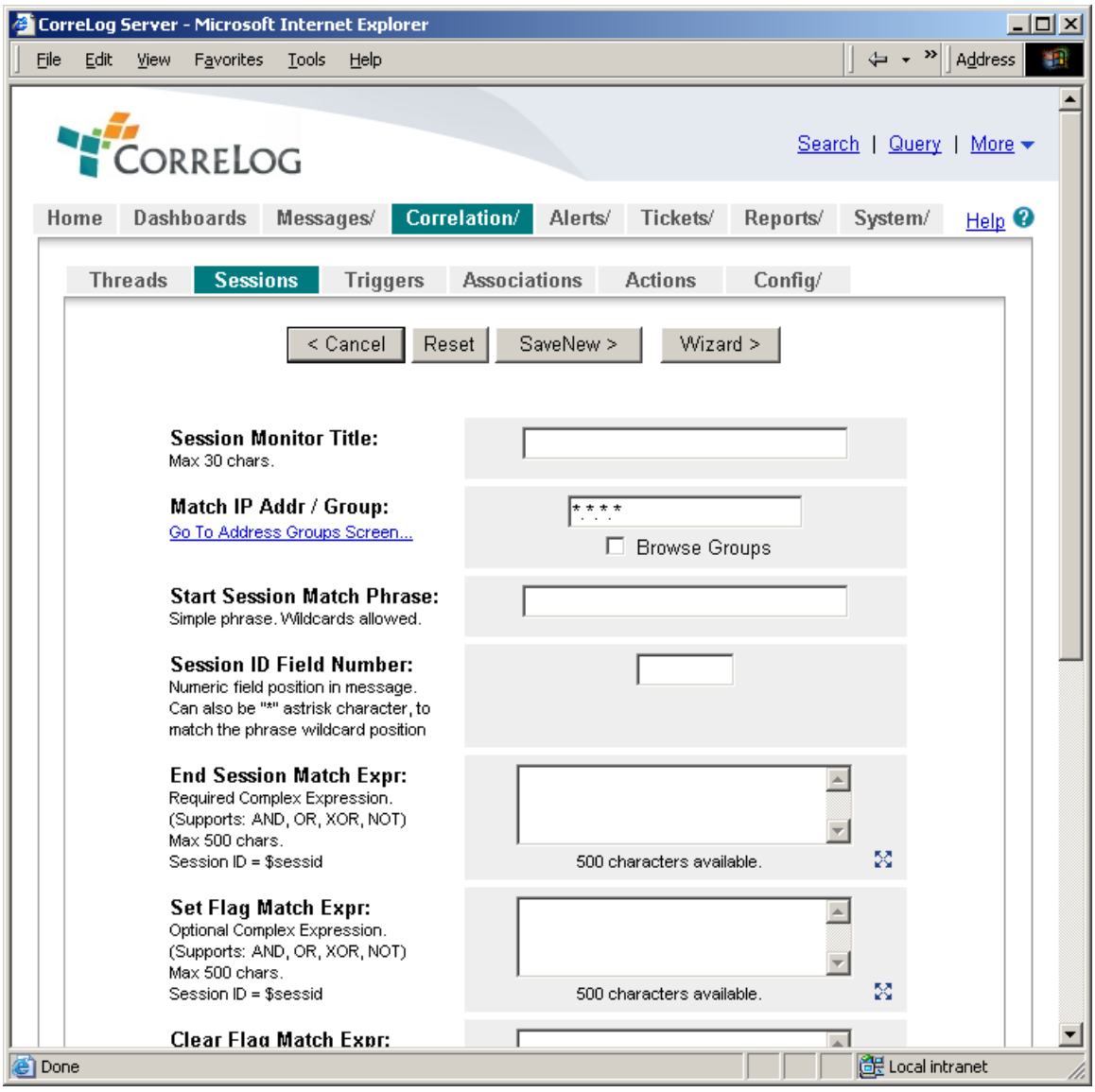
- **Session Count.** Each session monitor reports the count of sessions currently active for the monitor, at the far right of the session monitor title. This number represents the total number of sessions that are running on the system.

- **Total Monitored Sessions Status Message.** Towards the bottom of the screen is a total running count of all sessions on the screen. Note that the maximum number of sessions across all monitors is limited to 50,000 (or some other value configured by CorreLog support.) The system cannot exceed 100% capacity, as reported by the status message at the bottom of the screen.

- **Audit Session Link.** Towards the bottom of the screen is a link that permits the user to audit all the session parameters on the system. This link is useful for auditors that require an overview of the parameter settings for each session monitor.

Session Monitor Configuration Items

Clicking on the "Add New" button, or "Edit" button for a session monitor displays the configuration screen for the session monitor. This screen defines the parameters of the session monitor, including the parsing rules and other parameters needed to track sessions. The "Add New" screen and "Edit" screens are similar, as depicted below:



Each session has the following data elements that must be configured and can be subsequently changed after a session monitor entry is created.

The "AddNew", and "Edit" screens are standard CorreLog dialogs, containing standard buttons such as "Save", SaveNew", "Cancel", "Reset", and "Delete"

buttons. The various data items for the "AddNew" and "Edit" dialogs are described below:

- **Session Monitor Title.** This value is an arbitrary string of fewer than 30 characters that identifies the particular session. The value appears in any messages related to the session, and also appears on the top-level "Sessions" screen.

- **Match IP Address / Group.** This value is an IP address or group name that limits the session to one or more distinct computers. By default, the session monitor matches messages from any device. The operator can specify a specific address or group to limit the session to a particular type of machine (such as "Server Farm Login Sessions".)

- **Start Session Match Phrase.** This is a simple match expression that identifies the "start message". The value cannot be a full expression, but must be a single keyword or wildcard. The start message must contain a particular field of interest that can be parsed from the message. (The field is identified in the "Session ID Field Number" value, discussed below.)

- **Session ID Field Number.** This value is either a number or an asterisk (*) character. If the value is a number, it identifies the particular word in the "start message" that will be used as the session ID. If the value is an asterisk (*) character, the word in the start message is identified by the first word matched by the asterisk in the "start message". For example, if the fifth word in the start message is always the user name, then the value of this field is "5". (See additional examples below.)

- **End Session Match Expression.** This is a match expression that identifies the "end message" and the end of the session. The value usually includes the special "$sessid" value, which is substituted for the session ID parsed from the above two values. (See additional notes below.)

- **Set Flag Match Expression.** This is an optional match expression that can be used to set a flag for the session. This value is completely optional. If any message is found from the session IP address that matches this expression, the flag is set. The actually application of the flag is at the discretion of operator. This value is mainly useful when updating sessions in a relational database, as described in a later section.

- **Clear Flag Match Expression.** This is an optional match expression that can be used to clear the flag for the session. This value is completely optional. As above, the actual application of flags is at the discretion of the operator, and the value is mainly useful when updating sessions in a relational database, as described later.

- **Increment Count Match Expression.** This is an optional match expression that increments a session counter. This counter is optional, but is generally configured to match the "$sessid" value, so as to count the number of messages related to the particular session. The value can be used as an activity counter to indicate how active the session is or has been.

- **End Session Message Severity.** This value indicates the severity of the message that is sent back to CorreLog. When the "end session" message occurs, the session monitor sends a standard message (with the severity specified here) back to CorreLog, where it can be further correlated and reported upon.

- **Session Error Message Severity.** This value indicates the severity of the message that is sent back to CorreLog when an error occurs. The principle error message (which uses this severity) is a message indicating that a session has restarted without first receiving an "end message" indication.

The Special $sessid Variable

The CorreLog Session Monitor is unique in that it keeps track of multiple "Session ID" values. For each session monitor entry, there can exist multiple active sessions. Each session has its own particular $sessid" value. Stated slightly differently, the unique capability of the Session Monitor is that it can track multiple simultaneous states

The "Session ID" is a single word that is in common between the "start message" and the "end message". The Session ID is typically a username, but can be some other value such as a node and port number, a particular status value, or any single word that appears in both the start and end messages"

Within the context of the session, the "$sessid" value is immediately replaced by whatever value was parsed from the start message. The operator includes the "$sessid" value in the "End Session Match Expression", the "Set Flag Match Expression", the "Clear Flag Match Expression" and / or the "Increment Count Match Expression".

Basic Configuration Example

For example, consider a "session start message: as follows:

```
Session started for User0001
```

The user configures the "Start Session Match Phrase" and "Session ID Field Number" to capture the value of User0001 as the Session ID. If any message is

received that matches the configured "Match Phrase" a session entry is created. The value of the user name (parsed from the message) is assigned to $sessid". Specifically, the match phrase is "Session Started", and the "Session ID Field Number" is "4" (to identify the Session ID as the fourth word of the message.)

Continuing the above example, consider the session ends with a message as follows:

```
Session ended for User0001
```

To match this exact message and end the session, the user specifies the "End Session Match Expression" with a value such as "Session ended for $sessid", which will precisely match the end message for the particular user (and not for "User9999", or some other user.)

Using this technique, the operator can not only track the start and end messages for a session, but can additionally match other message set flags, clear flags, or increment the session activity counter. This is accomplished by incorporating the $sessid" value into any of the other match expressions for the particular session monitor entry. For example, to count the number of messages that occur between the start and end messages (which contain the user name) the operator configures the "Increment Count Match Expression" to be the value "$sessid".

Session Data Browsing

Actual Session data is available by clicking on the "Active Sessions", "History", or "Graphs" links on the top-level screen. This presents data in tabular or graphical format, which allows the user to search for individual columns of data, as well as inspect detailed information about each session.

The "Active Sessions" data consists of five columns of data:

- **Detail Button.** The user can click on the "Detail #NN" button to view details regarding the individual session. This function can also be used to selectively delete a session item.

- **Start Time.** The second column of the table indicates the time that the session was started, including the elapsed time from the present time.

- **Update Time.** The third column of the table indicates the time that the session was updated, including the last time from the present time.

- **Session Address.** The fourth column of the table indicates the session address, i.e. the IP address of the start message. The user can search for particular values using the match expression at the top of the column, to limit the display to a particular IP address.

- **Session ID.** The fifth column of the table indicates the session identifier parsed from the start message, uniquely identifying this particular session. The user can search for particular values using the match expression at the top of the column, to limit the display to a particular session ID.

- **Message Count.** The last column of the table indicates the number of messages that have been received for this session, since the session was first added to the system.

External Session Data / Program Interface

Finally, the above data is reflected into a text file that can be used for advanced features. The session data resides in the "./stat/sess.stt" file of the CorreLog system. The "sess.stt" file consists of various columns that contain the complete session data of the system, documented elsewhere. Note that this file is limited to 50,000 lines, which is the maximum number of sessions that the system can maintain using standard parameters.

This "./stat/sess.stt" file can be used by programmers to extend the range of correlation, such as via the "Custom Alerts" facility of the CorreLog system. This data can further be reflected into a relational database, as discussed in the next section.

Section 4: Advanced Usage

The previous section provided an overview of operation that will typically be sufficient to completely operate the CorreLog Session Monitor software, including the ability to configure sessions using both simple and advanced techniques. This new section herein elaborates on this information, providing additional information on several advanced features (available via the "Advanced" button on the top-level screen).

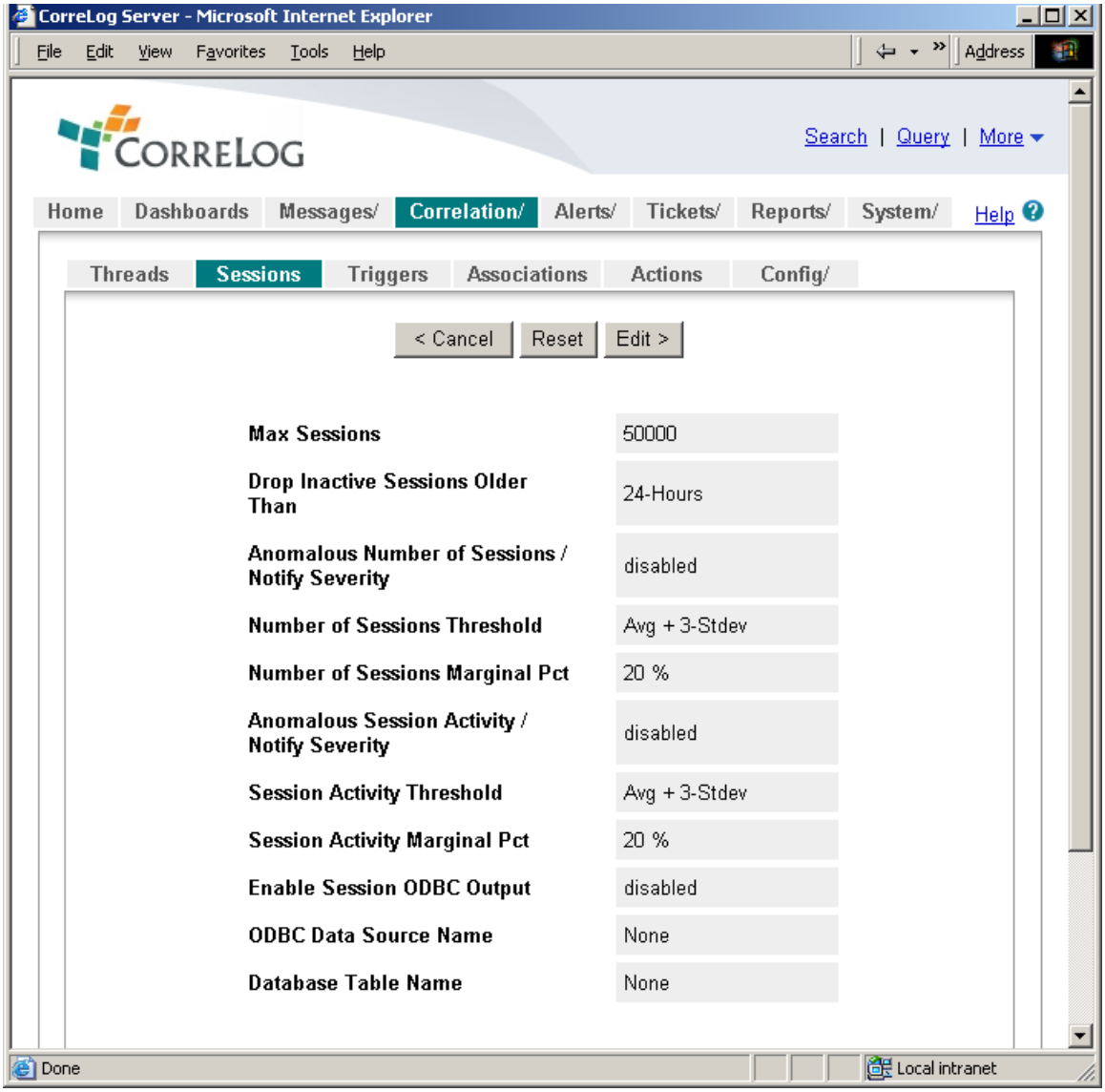
These more advanced features allow the system to perform additional functions, such as automatic statistical analysis of sessions for outlier's and anomaly detection. These functions can also be useful for exporting data to a relational database for more analysis and reporting.

Note that anomaly detection, described in this section, consists of comparing session data (in a fully automated fashion) to data as a whole, detecting when some aspect of the data (such as counts) exceeds several standard deviations of magnitude beyond the average. This may indicate a particularly strange session, such as a user logging into a platform more than typically expected. These situations can automatically be detected by the software and can open CorreLog tickets and trigger notifications.

This section provides a description of the advanced features of the system, and the various configurable parameters. The information in this section will be of interest to advanced system users, as well as administrators looking for ways to further leverage the session data collected by CorreLog.

Advanced Functions Screen

The advanced function screen is accessed by clicking on the "Advanced" button at the top of the "Correlation > Sessions" screen. This button is normally accessible only to "admin" type CorreLog users. The Advanced Configuration screen is depicted below.


CorreLog Server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address
CORRELOG
Search | Query | More
Home Dashboards Messages/ Correlation/ Alerts/ Tickets/ Reports/ System/ Help
Threads Sessions Triggers Associations Actions Config/
< Cancel Reset Edit >
Max Sessions 50000
Drop Inactive Sessions Older Than 24-Hours
Anomalous Number of Sessions / Notify Severity disabled
Number of Sessions Threshold Avg + 3-Stdev
Number of Sessions Marginal Pct 20 %
Anomalous Session Activity / Notify Severity disabled
Session Activity Threshold Avg + 3-Stdev
Session Activity Marginal Pct 20 %
Enable Session ODBC Output disabled
ODBC Data Source Name None
Database Table Name None
Done
Local intranet

The above screen is a standard CorreLog parameters dialog. The user returns to the previous screen via the "Cancel" button. The user edits parameters by clicking the "Edit" button. The "Reset" button refreshes the screen with the latest data, and the "Wizard" function can be used to add a new session (identical to the "Wizard" button on the top-level screen.

The various parameters of this screen are described below.

- **Max Sessions.** This value is the maximum number of sessions available to the system, and is not changeable by the end-user. This value can be modified only by CorreLog support. The value is included on this screen strictly for reference.

- **Drop Inactive Sessions**. This value indicates how long a session that has not been updated is maintained by the system. If a session has not been updated in the period of time specified here (by default 24-hours) the session is removed, cleaning the table, and providing additional space for new entries.

- **Anomalous Number of Sessions.** This value indicates the severity of the message issued when an "anomalous number of sessions" condition is detected on the system. The default value is "disabled", indicating no message is sent.

- **Number of Sessions Threshold.** This value is the threshold for the anomalous number of sessions. By default, if the session count for any session item is more than three standard deviations away from the average number of sessions, this condition is detected and reported.

- **Number of Sessions Marginal Pct.** This value is a secondary threshold for the anomalous number of sessions. The number of sessions must exceed this percentage of the average (in addition to lying outside the threshold above.

- **Anomalous Session Activity Severity.** This value indicates the severity of the message issued when the number of messages related to a particular session item falls above the configured threshold. The default value is "disabled", indicating no message is sent.

- **Session Activity Threshold.** This value is the threshold for the anomalous session activity. By default, if the number of messages for any session item is more than three standard deviations away from the average number of messages, this condition is detected and reported.

- **Session Activity Marginal Pct.** This value is a secondary threshold for the anomalous session activity. The number messages for an session must exceed this percentage of the average (in addition to lying outside the threshold above.)

- **Enable Session ODBC Output.** This value enables the automatic output of session data to a relational database table and ODBC Data Source,

configured below. This provides a simple method of exporting all session data to a relational database for further reporting and analysis.

- **ODBC Data Source Name.** This value is an ODBC data source name (configured on the CorreLog "System > ODBC" screen) that will receive the session data. The user should configure the ODBC data source in the Windows control panel as a system DSN, and then configure the value in the "System > ODBC" screen for the data item to appear in this drop-down list.

- **Database Table Name.** This is the database table name that receives the session data. In order to update data into a relational database, the operator must (1) enable the Session ODBC Output; (2) select the ODBC Data Source Name; and (3) then specify a valid Database Table Name here.

Statistical Anomaly Detection

The statistical anomaly detection runs at midnight, so any messages indicating an anomalous condition will appear at that time, unless the facility is specifically bypassed by setting the message severity to "disabled" for the anomaly detection, or setting the threshold to a very high value.

Note that the "Advanced" screen provisions two different and distinct types of anomalies, and looks for two separate indicators of anomalous behavior. These indicators, while appearing similar, are actually quite different:

- **Anomalous Number of Sessions.** This condition exists when any session address has more sessions than the average number of sessions for all entries. Generally, this may indicate a security risk because a user has excessive and unnaturally large numbers of sessions, such as the user is logging into too many platforms of different types.

- **Anomalous Session Item Activity.** This condition exists when any session item has more messages than the average number of messages for any item. The message counts are displayed on various screens, and indicate how often the session is actually updated on the system. Generally, this may indicate a security risk because the user is generating an exceptional number of messages, hence may be performing some malicious or suspicious act.

When one of these conditions occurs, the system sends a message for each detected condition of the severity specified on the "Advanced" screen. The exact format of the message appears in Appendix A of this document.

Database Updates Configuration Procedure

Session data is located in tabular format within the "./stat/sess.stt" file of the system, permitting developers to script custom applications for advanced correlation of this data. For example, a programmer (or CorreLog support) can create "Custom Alerts" that periodically check this data and provide useful detections for highly specialized applications.

In addition to this file, the session data can be directly loaded into a relational database table, permitting sophisticated queries using standard SQL, possibly for advanced anomaly detection, or simply for reporting purposes. This feature is easy to initialize as follows:

1. The administrator creates an ODBC data source using the Windows Control Panel > Admin Tools. In the absence of any particular database, the administrator can use a MS Access database.

2. The administrator configures the ODBC data source using the CorreLog "Reports > ODBC" tool. This step configures the user name, password, database name, and other parameters needed for CorreLog to communicate with the database.

3. On the "Correlation > Sessions > Advanced" screen, the administrator enables the ODBC output, selects the ODBC data source configured above (which will now appear in the drop down menu of ODBC data sources) and specifies a database table.

No further configuration is necessary. CorreLog will automatically create an appropriate table (of the user selected name), and begin populating this table with new session data. Additionally, the table will automatically be truncated when any session older than N days exists, limiting the size of the table and conserving disk space.

The actual database table, created and maintained by the system, consists of eight columns, as follows:

Ident (Varchar(16))

This column contains the "Session Identifier" for the particular session monitor. The identifiers are displayed by the "Audit Full Session Data" screen, accessed via a hyperlink at the bottom of the "Correlation > Sessions" screen. The identifier uniquely identifies each session monitor in the system, and normally consists of a twelve digit numeric string.

Address (Varchar(16))

This column contains the IP address of the session.

Session_(D (Varchar(50))

This column contains the Session ID, and consists of 50 characters or less. This is the username of the session or other unique Session ID value.

Start_Time (Varchar(22))

This column contains a text string in ISO time format, which indicates the time that the session item was first created on the system. This value is used to drop the session after N-days of non-activity.

Last_Update (Varchar(22))

This column contains a text string in ISO time format, which indicates the time that the session item was last updated on the system. This value is used to drop the session after N-days of non-activity, and is useful for indicating how recently the session was updated.

Flags (Integer(10))

This column contains a count of the flagged messages that have occurred on the system for the particular session.

Count (Integer(10))

This column contains a count of the messages that have occurred on the system for the particular session. The value indicates the "Session Activity", and indicates how often this particular session occurs on the system.

Elapsed (Integer(10))

This column contains the elapsed time of the session in seconds, and indicates the difference between the start and elapsed time

Using the above table, reports can be generated that indicate items such as session counts, session activity, and other profile information that may be useful for highly specific correlation.

For Additional Help…

Detailed specifications regarding the CorreLog Server, add-on components, and resources are available from our corporate website. Test software may be downloaded for immediate evaluation. Additionally, CorreLog is pleased to support proof-of-concepts, and provide technology proposals and demonstrations on request.

CorreLog, Inc., a privately held corporation, has produced software and framework components used successfully by hundreds of government and private operations worldwide. We deliver security information and event management (SIEM) software, combined with deep correlation functions, and advanced security solutions. CorreLog markets its solutions directly and through partners.

We are committed to advancing and redefining the state-of-art of system management, using open and standards-based protocols and methods. Visit our website today for more information.

CorreLog, Inc.
http://www.CorreLog.com
mailto:support@CorreLog.com

Alphabetical Index

A

Access / 27
Active / 11 12 16 20
Activity / 25 26 28
Actual / 9 20
Adapter / 31
Addnew / 13 14 15 17 18
Address / 6 18 20 27
Admin / 27
Administrative / 9
Administrator / 10
Advanced / 13 15 23 24 26 27
Advanced Usage / 23
Agent / 14
Alerts / 8 11 21 27
Alphabetical Index / 31
Anomalous / 25 26
Anomaly / 26
Anomaly, Statistical Detection / 26
Apply / 15
Audit / 16 27

B

Background / 6

Basic / 9 19
Basic Configuration Example / 19
Beneath / 15
Browsing / 13 20
Browsing, Session Data / 20
Button / 15 20

C

Cancel / 17 24
Checkout / 11
Checkout, Preliminary And Test Procedure / 11
Clear / 18 19
Clicking / 17
Co-catlogexe / 7
Co-devlogexe / 7
Co-sessexe / 7
Collection / 13
Configuration / 13 17 19 24 27
Configuration, Basic Example / 19
Continuing / 20
Correlation / 5 6 7 9 11 14 24 27
Count / 15 16 19 20 21 28
Custom / 8 21 27

D

Data / 13 15 20 21 25 26 27
Data, Session Browsing / 20
Data, Session Table / 15
Database / 26 27
Delete / 17
Detail / 20
Detailed / 29
Detection / 13 26
Detection, Statistical Anomaly / 26
Disk / 10
Distribution / 9
Drop / 25

E

Elapsed / 28
Enable / 25
Error / 19
Example / 19

Example, Basic Configuration / 19
Existing / 10
Expression / 18 19 20
External / 21

F

Farm / 18
Field / 18 19 20
Flag / 18 19
Flags / 28
Framework / 10
Full / 27
Functions / 13 15 24

G

Generate / 11
Graphs / 16 20
Group / 18

H

History / 12 16 20
How To Use This Manual / 8

I

Identifier / 27
Inactive / 25
Increment / 19 20
Index / 31
Index, Alphabetical / 31
Information / 6
Installation / 9 10
Installation, Software / 9
Installation, Windows Procedure / 10
Interface / 21
Introduction / 5 5
Item / 26
Items / 17

L

Last update / 28
Link / 16

Links / 16
Logout / 11
Logout, User Test000 / 11

M

Manager / 10 11
Manual / 8 10
Manual, How To Use This / 8
Marginal / 25
Message / 9 11 16 19 21
Messages / 9 11
Mode / 15
Monitored / 16

N

N-days / 28
Name / 11 15 26
Number / 18 19 20 25 26

O

Odbc / 25 26 27
Operation / 6 13
Operation, Session Monitor / 6
Operation, Software / 13
Output / 25
Overview / 7
Overview, Process / 7

P

Page / 31
Pattern / 15
Phrase / 18 19 20
Plug-in / 5
Post / 9 11
Preliminary / 11
Preliminary Checkout And Test Procedure / 11
Procedure / 10 11 27
Procedure, Preliminary Checkout And Test / 11
Procedure, Windows Installation / 10
Process / 7
Process Overview / 7
Program / 21

R

Reference / 10
Reports / 27
Requirements / 10
Reset / 17 24
Restart / 10

S

Save / 17
Savenew / 17
Schedule / 7
Search / 9 11
Server / 5 10 18 29
Service / 10
Session Data Browsing / 20
Session Data Table / 15
Session Monitor Operation / 6
Sessions / 5 6 7 9 11 12 14 15 16 18 20 24 25 26 27
Severity / 19 25
Software / 9 13
Software Installation / 9
Software Operation / 13
Sort / 15
Source / 25 26
Space / 10
Start / 18 19 20
Start time / 28
Started / 20
Stated / 19
Statistical / 26
Statistical Anomaly Detection / 26
Status / 16
Syslog / 8
System / 7 26

T

Table / 15 26
Table, Session Data / 15
Task / 10 11
Test000 / 11 12
Test000, User Logout / 11
Threshold / 25

Time / 15 16 20
Title / 15 18
Tools / 27
Top-level / 14
Total / 16
Towards / 16

U

Update / 20
Updated / 16
Updates / 27
Usage / 23
Usage, Advanced / 23
User / 8 10 11
User0001 / 19 20
User9999 / 20
User Logout Test000 / 11
Users / 11

V

Variable / 19
Verify / 11 12
Visit / 29
Vista / 10

W

Windows / 7 9 10 11 13 26 27
Windows Installation Procedure / 10
Winzip / 9
Wizard / 13 14 15 24